POSTAL METHODS AND SYSTEMS EMPLOYING DIGITAL WATERMARKS

Sub a1

Related Application Data

The subject matter of the present application is related to that disclosed in U.S. Patent 5,862,260, and in copending applications 08/746,613, filed November 12, 1996 (allowed); 09/074,034, filed May 6, 1998; 09/127,502, filed July 31, 1998; 09/185,380, filed November 3, 1998; 09/234,780, filed January 20, 1999; 09/287,940, filed April 7, 1999; 09/314,648, filed May 19, 1999; 09/343,104, filed June 29, 1999; 60/158,015, filed October 6, 1999; 09/433,104, filed November 3, 1999; 60/164,619, filed November 10, 1999; 09/503,881, filed February 14, 2000; 09/525,865, filed March 15, 2000; 09/547,664, filed April 12, 2000; 09/562,516, filed May 1, 2000; and 09/562,524, filed May 1, 2000.

The present application is a continuation-in-part of applications 09/567,405, filed May 8, 2000, 09/314,648, filed May 19, 1999, and 09/343,104, filed June 29, 1999.

Background and Summary of the Invention

Computer printers have long been used to print addresses on envelopes. For many years, a variety of similar printing technologies have been used to print metered postage on envelopes. With the advent of digital postage, use of printers with envelopes is increasing still further.

Digital postage technology is available from a number of vendors including Pitney Bowes, E-Stamp, Stamps.com and Escher Laboratories (of Escher Group, Ltd.), and is detailed in various patent publications including 5,982,506, 5,825,893, 5,819,240, 5,801,364, 5,774,886, 5,682,318, 5,978,781, and WO 99/18543A1.

Digital watermarking technology is used, in accordance with the present invention, to increase the security of, and augment the functionality associated with, computer printing of envelopes and postage.

In accordance with one aspect of the invention, traceability of digital postage is enhanced by serialization, i.e., embedding a serial number code or other indicia that uniquely and covertly links the printed postage to some device in the users' possession.

This device can be a printer, personal computer, or hardware security device used in printing the postage. In an exemplary embodiment, digital watermarking of the sort detailed in the cited patents and applications is used to embed the code at the time the postage is printed. The embedded data would only be detectable to investigators equipped with special readers for spot checking documents or investigating counterfeits.

Duplicate fraud is threat to metered and PC-postage systems. In this form of fraud, the criminal reproduces original printed postage and attaches it or prints it onto one or more additional mail pieces. In accordance with another aspect of the invention, security of metered or PC-printed digital postage against reproduction is enhanced through use of "fragile" digital watermarks. (A "fragile" digital watermark is one designed to evidence the scanning/printing operations associated with reproduction, such as photocopying or PC-based scanning and printing.) Such a watermark may be employed to provide forensic evidence that printed postage is not original.

In accordance with yet another aspect of the invention, watermark technology is employed to prevent – outright – the photocopying or other duplication of digital postage. This result is achieved by encoding on envelopes or in a digital postage indicia a "do not copy" watermark to which photocopiers, scanners, printers, and other computer devices or software are alert. If such a watermark is encountered, the device will refuse to operate, or will otherwise interfere with the reproduction operation.

In accordance with still another aspect of the invention, watermarking on an envelope is employed as an element of a franking mark (postal mark) – one that may stay within or extend well beyond the corner location typically associated with such marks.

In accordance with yet another aspect of the invention, watermarking on an envelope can serve as a portal to a corresponding internet site or internet-based application. That is, a printed document with an embedded watermark can be held up to a web cam, or scanned by a scanner, and instantly link a user to Internet sites or applications. Importantly, information received in this manner is not subject to the delays associated with physical mail delivery, but can convey up-to-the-minute information.

In accordance with still another aspect of the invention, an envelope watermark serves to convey an identifier that is used to access associated data in a database. In one

particular application, the index number identifies the recipient. Thus, for example, an envelope can be addressed simply by watermarking it with a unique recipient designator, e.g., JOHNQPUBLIC843. Processing equipment in the postal system can read the watermark, query a database with the designator, and determine thereby the recipient's physical address. (If desired, the address thereby discerned can be printed on the envelope.) One advantage to this arrangement is that distribution of Change of Address cards would be a thing of the past. If a person moves across country, a single record in the database is changed. All mail to that recipient automatically is directed to the new physical address. Further, a recipient could temporarily redirect mail delivery, including optional electronic delivery of certain items.

The features just-described can be employed alone or in various combinations.

The foregoing and additional features and advantages of the present invention will be more readily apparent from the following detailed description.

Detailed Description

Digital watermarking technology, a form of steganography, encompasses a great variety of techniques by which plural bits of digital data are hidden in some other object without leaving human-apparent evidence of alteration or data representation.

Digital watermarking of envelopes can be effected in numerous ways, including by ink, by texturing, by laminate layers, etc. (As used herein, envelope is meant to include any item of mail, including cards, catalogs, etc., having postage directly printed thereon, or to which postage is affixed, e.g., by a label.) The watermarking can be formed as part of other markings on the envelope (e.g., franking marks, graphics, text, etc.), or can be applied irrespective of such other markings. Watermarking can be effected at any time in an envelope's life, including at the time of media-making (e.g., paper making or Tyvek formation), at the time of envelope making, at the time of consumer use (either before, during, or after the application of other envelope markings), and thereafter (e.g., in the course of postal service processing).

The watermarking may span all of one side (or both sides) of an envelope, or may be localized, e.g., in the areas typically associated with postage, return address, and

recipient address. An envelope may convey a single watermark, or several may be used, e.g., conveying different information or serving different purposes in different regions. Several different watermarking technologies can be employed on a single envelope, e.g., the envelope's texture can convey one type of information, and tinting printed on the envelope can convey a second type of information. Moreover, both the front and back of the envelope can be encoded – either with the same watermark information or different. Still further, the inside of the envelope or mail piece (e.g., catalog) can likewise be encoded. The watermark may be formed in an otherwise blank area, or can be integrated into other graphics, such as advertising artwork, corporate logos, etc.

Sub a2 Any print- or physical media-watermark technology can be employed in conjunction with the present invention. Representative watermarking technologies suitable for such use are detailed in the assignee's patent 5,862,260, and in applications 09/074,034, 09/127,502, 09/503,881, 09/562,516, and 09/562,524. A great many other watermarking technologies are familiar to those skilled in the digital watermarking art.

In accordance with one aspect of the invention, traceability of digital postage is enhanced by serialization, i.e., embedding a serial number code or other indicia that uniquely and covertly links the printed postage to some device in the users' possession.

In one such embodiment, the watermark serves to convey an identifier of a printer, personal computer, postage vault, or other device used in printing postage. The identifier can be a registration number, a serial number, an account number, etc. Other forensic information can likewise be encoded.

The encoded information can directly correspond to the device, or the relationship can be established through a remote database (e.g., the identifier can be an index number that, when looked-up in a database, yields the registered owner name and address of a particular device).

Typically, such a watermark is "private," i.e., it is readable only to selected classes of persons who have access to secret data, such as a private key. Postal investigators and the like would be able to read such data (e.g., by using a specialized reader system, or by using a conventional reader system equipped with the private information), but the general public would not. Such a security watermark (fragile or

robust) may also be read by mail processing equipment, such as sorting machines, either on a continuous- or spot-checking basis, either for the purpose of security checking or for the purpose of routing.

In other embodiments, the watermark is public, but general use thereof is limited because a database needed to interpret the encoded data is not publicly accessible.

As indicated above, this forensic watermark can take various forms. For example, it can form part of the franking indicia printed on the envelope, or can be separate from such indicia. It can be limited to the franking corner of the envelope, or can be located in a different location, or span a larger area. One particular implementation deposits a light splattering of tiny ink droplets over an area. These droplets are sufficient to form a computer-detectable pattern, but are not conspicuous (or preferably even visible) to human observers. In this, and other embodiments, the invisibility of the markings can be enhanced by using inks responsive to ultraviolet or infrared illumination, or inks that are less perceptible to the human, such as yellows as more particularly detailed in the earlier cited applications.

In most applications, the forensic watermark is applied automatically as part of another envelope processing activity. Thus, for example, such functionality can be provided in software used to print addresses on envelopes, or apply digital postage to envelopes. The software can be of the consumer variety (e.g., Microsoft Word or a digital postage application), or it can be system or device instructions invoked as part of the printing operation (e.g., printer driver software, or firmware associated with a printer's microprocessor.) As the user-intended information is being printed, the forensic marking is also being applied. Thereafter, if an issue arises as to the source of an envelope, or postal indicia thereon, the forensic information can be checked to aid in such investigation.

In accordance with a second aspect of the invention, security of digital postage against reproduction is enhanced through use of "fragile" digital watermarks.

As noted, a "fragile" digital watermark is one designed to evidence copying (e.g., by not surviving, or by having attributes that change in a detectable manner during the scanning/printing operations associated with copying)not to withstand the

scanning/printing operations associated with photocopying. (The use of fragile watermarks is detailed in applications 09/433,104 and 09/234,780.) If markings (e.g., legitimate franking indicia) incorporating such a watermark are photocopied or otherwise reproduced from one envelope onto a second envelope, the copy will either not include the watermark or the watermark will be changed in a way that indicates it is a copy. Processing equipment in the postal system can be alert to such copies (which are identified by the absence or modification of the fragile watermark), and cull them from the properly-franked mail. Likewise, fraud or counterfeit investigators can use special readers to verify originality and detect copies.

A watermark may be made fragile in numerous ways. One form of fragility relies on low watermark amplitude. That is, the strength of the watermark is only marginally above the minimum needed for detection. If any significant fraction of the signal is lost, as typically occurs in photocopying operations, the watermark becomes unreadable.

Another form of fragility relies on the watermark's frequency spectrum. High frequencies are typically attenuated in the various sampling operations associated with digital scanning and printing. Even a high amplitude watermark signal can be significantly impaired, and rendered unreadable, by such photocopying operations.

The foregoing are but two of many different approaches. The particular fragile watermark used can be tailored in accordance with the type of scanning and printing anticipated in unauthorized reproduction.

As indicated, processing equipment in the postal system can routinely scan envelopes bearing digital postage for the presence of the expected fragile watermark. Any envelopes found to be missing the watermark can be culled for investigation.

In accordance with a third aspect of the invention, watermark technology is employed to prevent – outright – the photocopying or other duplication of digital postage. This result is achieved by encoding on envelopes a "do not copy" watermark to which photocopiers, scanners, printers, imaging software, or other computer devices are alert. If such a watermark is encountered, the device will refuse to operate, or will otherwise interfere with the reproduction operation.

Sub Q4

Such watermark-based "do not copy" systems are further detailed in applications 09/074,034, 09/127,502, 09/185,380 and 09/287,940. The detection of the watermark can occur in various, and preferably numerous, locations in likely reproduction systems. In a desktop computer system, for example, image data may be analyzed for such a watermark by software in the scanner (e.g., scanner driver software), software in the computer (e.g., TWAIN interface software, operating system software, image editing software, internet browser software, printer driver software), and software in the printer (e.g., printer firmware). If any of these detectors encounters image data that has a "do not copy" watermark encoded therein, the detector will interfere with its reproduction (e.g., by discontinuing the process, by scarring the image, by hiding tracer data for later forensic use, etc.)

The use of a watermark to indicate that an indicia should not be copied is desirable, but not necessary. Other hallmarks can be employed. For example, devices used in reproduction can be alert to the franking indicia itself and, if encountered, interfere with duplication.

In accordance with a fourth aspect of the invention, security is enhanced by associating (cryptographically or otherwise) a digital watermark formed on envelope stock (e.g., by printing or texturing) with data conveyed in a postal franking mark (e.g., a 2D bar code). In such case, for example, the envelope can be authorized for use only in conjunction with a certain printer, a certain postal meter, a certain postal account, a certain software, etc. If the envelope stock is diverted to another use (e.g., used in conjunction with a different postal meter), the discrepancy in the association between the envelope watermark and the postal franking mark can be detected by the postal authorities, and suitable action taken (e.g., alerting the proper owner of the envelope stock of such use).

The association between the envelope watermark and the postal indicia can be self-contained (e.g., the association can be demonstrated without reference to external resources), or a remote resource can be employed (e.g., a database can specify that envelope stock X should only be encountered with digital postage from account Y).

In a variant embodiment, a franking station can check the watermark already existing on an envelope prior to applying postage. If a correct watermark is not detected, the franking station can decline to apply postage absent supervisory clearance. Unauthorized use of corporate mail accounts for use on personal correspondence may thereby be curbed.

In accordance with a fifth aspect of the invention, watermarking on an envelope is employed as an element of a franking mark. Such marking can be confined to the corner location typically associated with postage, but need not be so limited. If the marking extends across the entire envelope – on one side or both – machine processing of the mail by the postal system can be facilitated by obviating the need for positioning the envelope in a certain orientation for reading. In one particular embodiment, an embedded calibration signal associated with certain watermarks (c.f., the cited patent documents) can be used to orient a digital image of the envelope for both watermark reading as well as for other machine processing.

To make clear to office personnel that postage has been applied to such an envelope, it is generally desirable that the marking be visible. This can be achieved by increasing the amplitude of the watermark signal so that it appears as a patterned tile (or other shape). Or the watermark can be imperceptible, and other indicia added to indicate that postage has been applied (e.g., text stating "Posted with $0.33, printed in the same area as the watermark, or in a different area).

In still other arrangements, a conventional 2D barcode franking mark is subtly changed to, itself, imperceptibly carry the watermark. Or a faint tinting can be applied to the franking indicia area, and modulated to carry the watermark.

The information encoded in the franking (or other) watermark can represent a great variety of data. The amount of postage encoded, the date of encoding, the sender's name, address and zip code, the recipient's name, address and zip code, etc., can all be indicated.

In some embodiments, all such information is directly encoded in the watermark. In other embodiments, the watermark encodes an abbreviated data set, e.g., including a code number. The code number corresponds to additional information that can be found

in a database record accessed by the code – either maintained by the user, by a central authority (e.g., the postal system), or by some remotely accessible database.

In accordance with a sixth aspect of the invention, watermarking on an envelope serves as a portal to a corresponding internet site or application (which could be local on the user's PC).

As detailed in applications 09/343,104 and 09/547,664, a watermarked document can be held up to a web cam, or scanned by a scanner, and serve to instantly link a user to an Internet site, to invoke an application, etc. An envelope marked in this fashion can allow a user to initiate an essentially unlimited range of options.

Consider an envelope having the sender's contact information (name, address, zip code, phone number, fax number, email address, etc.) represented by a watermark (either literally, or referring to a database record). A recipient of the envelope may present same to a web cam associated with a personal computer. The camera decodes the watermark, finds it is contact information for a person, and in response automatically adds the contact information to a contact organizer (e.g., Microsoft Outlook) maintained by the computer.

Different watermarks may trigger different reactions. Certain of the payload bits in the watermark may indicate the type of data represented, and/or the type of reaction that is appropriate. Responses may be programmed by the sender, so the watermark is the same, but the backend system that is linked to the watermark contains the programming for what response to invoke.

One type of watermark may indicate that the encoded information is contact information that is available for loading into a recipient's contact organizer. A second type of watermark may indicate that a delivery confirmation message is to be dispatched to the sender of the envelope. When such an envelope is presented to the receipient's web cam, the associated computer automatically composes an email message confirming delivery of the envelope, and sends it to an address represented in the watermark.

A third type of watermark may direct a web browser associated with the recipient's computer to a destination specified by the watermark. The destination web address can provide the recipient with additional information related to the mailing, but updated to the minute. Advertising mailings can thus link to ordering pages, new sale

promotions, updated backorder status information, etc. Utility bills can link to summary account information showing payments received or owing, month-to-date charges, etc. The linked web address may present a form soliciting input or response from the envelope recipient, including survey responses, votes, etc.

The linked resource needn't convey just textual or graphical information. Entertainment programming can be similarly invoked, e.g., the delivery of previews of tonight's cable television shows, popular music recordings for preview or purchase, etc.

A fourth type of watermark may initiate a replenishment of postage in the recipient's digital postage account.

The foregoing is just a small sampling of the myriad functions that can be invoked – locally in the recipient's computer, or employing remote resources (e.g., computers accessed over the internet) – in response to presentation of a mailing to a webcam or other imaging device.

Some watermarks may correspond to several alternative actions. In such case, the recipient's computer may present a menu from which the recipient can select the desired response. Or the response invoked by presenting the envelope to the web cam may be made dependent on context or environment in which the presentation is made (e.g., time of day, type of device to which web cam is connected – fixed or portable computer, wired or wireless, etc.)

In a variant of the foregoing embodiment, an envelope watermark serves to convey an identifier that is used to access a database record having information related to mail processing or delivery. In one particular application, the index number identifies the recipient. Thus, for example, an envelope can be addressed simply by watermarking it with a unique recipient designator, e.g., JOHNQPUBLIC843. Processing equipment in the postal system can read the watermark, query a database with the designator, and determine thereby the recipient's physical address (e.g., street address).

In some such embodiments, the physical address information obtained by this database lookup is printed on the envelope by the postal system for the benefit of the ultimate postal delivery person. In other embodiments, the postal delivery person is equipped with reader devices that make such printing superfluous.

As noted, an important advantage to this arrangement is that Change of Address cards would be a thing of the past. If a person moves across country, a single record in the database is changed. All mail to that recipient automatically is directed to the new physical address. A lifetime postal addressing system can thereby be realized.

It will be recognized that the arrangements described above can be combined and hybridized in various ways to economically effect multiple functionality.

To provide a comprehensive disclosure without unduly lengthening this specification, the patents and applications cited herein are incorporated herein by reference.

Having described and illustrated the principles of the invention with reference to illustrative embodiments, it should be recognized that the invention is not so limited.

For example, while digital watermarking typically does not leave any human-apparent evidence of alteration or data representation, certain of the foregoing applications do not require this. The markings used may be visible, and even conspicuous, without impairing essential functionality. Thus, bar codes, data glyphs, OCR markings, and other machine-readable indicia may be substituted, depending on the particular application requirements.

While the detailed embodiments were described with reference to desktop computers, it is recognized that such devices will increasingly be supplanted by other digital appliances, including general purpose personal digital assistants, multifunction cell phones, and specialized devices – many of which include integrated optical sensors (e.g., CCD or CMOS cameras). Moreover, the power and utility of the above-detailed embodiments and devices can be further enhanced by employing various wireless communications technologies, including the evolving Bluetooth standard.

The implementation of the watermark encoding and decoding systems is straightforward to artisans in the field, and thus not belabored here. Conventionally, such technology is implemented by suitable software, stored in long term memory (e.g., disk, ROM, etc.), and transferred to temporary memory (e.g., RAM) for execution on an associated CPU. In other implementations, the functionality can be achieved by

dedicated hardware, or by a combination of hardware and software. Reprogrammable logic, including FPGAs, can advantageously be employed in certain implementations.

While the specification makes reference to "paper" and "envelopes," these terms are used in shorthand fashion to refer to articles delivered by the postal service. Thus, postcards (e.g., direct mail cards) and Tyvek articles are meant to be encompassed by such references. Postcards may include multiple watermarks, e.g., a postal-related mark on the "address side," and a MediaBridge mark on the other. The two marks may be associated or linked in various manners.

Although not described in the context of existing postal meters, it should be recognized that the above-detailed technology is well-suited for implementation with such devices, as they generally use printing techniques that are suitable for digital watermark printing. By retrofitting existing postal meters, a great variety of security and marketing improvements can readily be provided.

The reader will recognize that a variety of additional security techniques can be employed in conjunction with the arrangements detailed above. For example, in some applications, it is useful to encrypt the message encoded in the watermark. Encryption provides an additional layer of security to prevent unwanted uses of the encoded information. Some examples of applicable cryptographic methods include RSA, DES, IDEA (International Data Encryption Algorithm), skipjack, discrete log systems (e.g., El Gamal Cipher), elliptic curve systems, cellular automata, etc.

These and other cryptographic methods can be used to create a digital signature to place in a watermark message. Public key cryptographic methods employ a private and public key. The private key is kept secret, and the public key is distributed. To digitally sign a message, the originator of the message encrypts the message with his private key. The private key is uniquely associated with the originator. Those users having a public key verify that the message has originated from the holder of the private key by using the public key to decrypt the message.

The message may be both encrypted and digitally signed using two stages of encryption. At the encoder, a digital signature stage encrypts at least part of the message with a private key. An encryption stage then encrypts the message with a public key.

The decoder reverses the process. First, a decryption stage decrypts the message with a private key corresponding to public key used in the encryption stage at the encoder. Then, a second stage decrypts the output of the previous stage with the public key corresponding to the private key used to create the digital signature.

Time and date stamping can be used in conjunction with encryption, or otherwise. Metadata can similarly be conveyed.

If desired, a watermark can be used to track mail (e.g., an envelope or parcel) through the delivery process. At various check points, a camera- or sensor-equipped device reads the watermark, extracts an identifier and logs the identifier along with additional information, such as location, time, etc. This information may be sent and maintained in a database that can be queried to determine the delivery status of the mail. Wireless devices can be employed to read watermarks and report status to a centralized or distributed database.

It should be recognized that the particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings with other teachings in this and the incorporated-by-reference patents/applications are also contemplated.

In view of the wide variety of embodiments to which the principles and features discussed above can be applied, it should be apparent that the detailed embodiments are illustrative only and should not be taken as limiting the scope of the invention. Rather, we claim as our invention all such modifications as may come within the scope and spirit of the following claims and equivalents thereof.